

ELLIPTIC CURVES, RANDOM MATRICES AND ORBITAL INTEGRALS

JEFFREY D. ACHTER AND JULIA GORDON

ABSTRACT. An isogeny class of elliptic curves over a finite field is determined by a quadratic Weil polynomial. Gekeler has given a product formula, in terms of congruence considerations involving that polynomial, for the size of such an isogeny class. In this paper, we give a new, transparent proof of this formula; it turns out that this product actually computes an adelic orbital integral which visibly counts the desired cardinality. This answers a question posed by N. Katz in [12, Remark 8.7].

1. INTRODUCTION

The isogeny class of an elliptic curve over a finite field \mathbb{F}_p of p elements is determined by its trace of Frobenius; calculating the size of such an isogeny class is a classical problem. Fix a number a with $|a| \leq 2\sqrt{p}$, and let $I(a, p)$ be the set of all elliptic curves over \mathbb{F}_p with trace of Frobenius a ; further suppose that $p \nmid a$, so that the isogeny class is ordinary.

Motivated by equidistribution considerations, Gekeler derives the following description of the size of $I(a, \mathbb{F}_p)$ ([8]; see also [12]). For each rational prime $\ell \neq p$, let

$$(1.1) \quad v_\ell(a, p) = \lim_{n \rightarrow \infty} \frac{\#\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^n) : \mathrm{tr}(\gamma) \equiv a \pmod{\ell^n}, \det(\gamma) \equiv p \pmod{\ell^n}\}}{\#\mathrm{SL}_2(\mathbb{Z}/\ell^n)/\ell^n}.$$

For $\ell = p$, let

$$(1.2) \quad v_p(a, p) = \lim_{n \rightarrow \infty} \frac{\#\{\gamma \in \mathrm{M}_2(\mathbb{Z}/p^n) : \mathrm{tr}(\gamma) \equiv a \pmod{p^n}, \det(\gamma) \equiv p \pmod{p^n}\}}{\#\mathrm{SL}_2(\mathbb{Z}/p^n)/p^n}.$$

On average, the number of elements of $\mathrm{GL}_2(\mathbb{Z}/\ell^n)$ with a given characteristic polynomial is $\#\mathrm{GL}_2(\mathbb{Z}/\ell^n)/(\#(\mathbb{Z}/\ell^n)^\times \cdot \ell^n)$. Thus, $v_\ell(a, p)$ measures the departure of the frequency of the event $f_\gamma(T) = T^2 - aT + p$ from the average.

It turns out that [8, Thm. 5.5]

$$(1.3) \quad \tilde{\#}I(a, p) = \frac{1}{2} \sqrt{p} v_\infty(a, p) \prod_\ell v_\ell(a, p),$$

where

$$v_\infty(a, p) = \frac{2}{\pi} \sqrt{1 - \frac{a^2}{4p}},$$

$\tilde{\#}I(a, p)$ is a count weighted by automorphisms (2.1), and we note that the term $H^*(a, p)$ of [8] actually computes $2\tilde{\#}I(a, p)$ (see [8, (2.10) and (2.13)] and [12, Theorem 8.5, p. 451]). This equation is almost miraculous. An equidistribution assumption about Frobenius elements, which is so strong that it can't possibly be true, leads one to the correct conclusion.

In contrast to the heuristic, the proof of (1.3) is somewhat pedestrian. Let $\Delta_{a,p} = a^2 - 4p$, let $K_{a,p} = \mathbb{Q}(\sqrt{\Delta_{a,p}})$, and let $\chi_{a,p}$ be the associated quadratic character. Classically, the size of the

JDA's research was partially supported by grants from the Simons Foundation (204164) and the NSA (H98230-14-1-0161 and H98230-15-1-0247). JG's research was supported by NSERC.

isogeny class $I(a, \mathbb{F}_p)$ is given by the Kronecker class number $H(\Delta_{a,p})$. Direct calculation [8] shows that, at least for unramified primes ℓ ,

$$v_\ell(a, p) = \frac{1}{1 - \frac{\chi_{a,p}(\ell)}{\ell}}$$

is the term at ℓ in the Euler product expansion of $L(1, \chi_{a,p})$. More generally, a term-by-term comparison shows that the right-hand side of (1.3) computes $H(\Delta_{a,p})$.

Even though (1.3) is striking and unconditional, one might still want a pure thought derivation of it. (We are not alone in this desire; Katz calls attention to this question in [12].) Our goal in the present paper is to provide a conceptual explanation of (1.3), and to extend it to the case of ordinary elliptic curves over an arbitrary finite field \mathbb{F}_q .

In a companion work, we will use a similar method to give an analogous product formula for the size of an isogeny class of simple ordinary principally polarized abelian varieties over a finite field.

Our method relies on the description, due to Langlands (for modular curves) and Kottwitz (in general), of the points on a Shimura variety over a finite field. A consequence of their study is that one can calculate the cardinality of an ordinary isogeny class of elliptic curves over \mathbb{F}_q using orbital integrals on the finite adelic points of GL_2 (Proposition 2.1). Our main observation is that one can, without explicit calculation, relate each local factor $v_\ell(a, q)$ to an orbital integral

$$(1.4) \quad \int_{G_{\gamma_\ell}(\mathbb{Q}_\ell) \backslash \mathrm{GL}_2(\mathbb{Q}_\ell)} \mathbf{1}_{\mathrm{GL}_2(\mathbb{Z}_\ell)}(x^{-1}\gamma_\ell x) dx,$$

where γ_ℓ is an element of $\mathrm{GL}_2(\mathbb{Q}_\ell)$ of trace a and determinant q , G_{γ_ℓ} is its centralizer in $\mathrm{GL}_2(\mathbb{Q}_\ell)$, and $\mathbf{1}_{\mathrm{GL}_2(\mathbb{Z}_\ell)}$ is the characteristic function of the maximal compact subgroup $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Here the choice of the invariant measure dx on the orbit is crucial. On one hand, the measure that is naturally related to Gekeler's numbers is the so-called *geometric measure* (cf. [7]), which we review in §3.1.3. On the other hand, this measure is inconvenient for computing the global volume term that appears in the formula of Langlands and Kottwitz. The main technical difficulty is the comparison, which should be well-known but is hard to find in the literature, between the geometric measure and the so-called *canonical measure*.

We start (§2) by establishing notation and reviewing the Langlands-Kottwitz formula. We define the relevant, natural measures in §3, and study the comparison factor between them in §4. Finally, in §5, we complete the global calculation. The appendix (§A), by S. Ali Altuğ, analyzes the comparison of measures from a slightly different perspective.

As we were finishing this paper, the authors of [6] shared their preprint with us; we invite the reader to consult that work for a different approach to Gekeler's random matrix model.

Notation. Throughout, \mathbb{F}_q is a finite field of characteristic p and cardinality $q = p^e$. Let \mathbb{Q}_q be the unique unramified extension of \mathbb{Q}_p of degree e , and let $\mathbb{Z}_q \subset \mathbb{Q}_q$ be its ring of integers. We use σ to denote both the canonical generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and its lift to $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$.

Typically, G will denote the algebraic group GL_2 . While many of our results admit immediate generalization to other reductive groups, as a rule we resist this temptation unless the statement and its proof require no additional notation.

Shortly, we will fix a regular semisimple element $\gamma_0 \in G(\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Q})$; its centralizer will variously be denoted G_{γ_0} and T .

Conjugacy in an (abstract) group is denoted by \sim .

Acknowledgment. We have benefited from discussions with Bill Casselman, Clifton Cunningham, David Roe, William Sawin, and Sug-Woo Shin. We are particularly grateful to Luis Garcia for sharing his insights. It is a great pleasure to thank these people.

2. PRELIMINARIES

Here we collect notation concerning isogeny classes (2.1) as well as basic information on Gekeler's ratios (2.3) and the Langlands-Kottwitz formula (2.4).

2.1. Isogeny classes of elliptic curves. If E/\mathbb{F}_q is an elliptic curve, then its characteristic polynomial of Frobenius has the form $f_{E/\mathbb{F}_q}(T) = T^2 - a_{E/\mathbb{F}_q}T + q$, where $|a_{E/\mathbb{F}_q}| \leq 2\sqrt{q}$. Moreover, E_1 and E_2 are \mathbb{F}_q -isogenous if and only if $a_{E_1/\mathbb{F}_q} = a_{E_2/\mathbb{F}_q}$. In particular, for a given integer a with $|a| \leq 2\sqrt{q}$, the set

$$I(a, q) = \left\{ E/\mathbb{F}_q : a_{E/\mathbb{F}_q} = a \right\}$$

is a single isogeny class of elliptic curves over \mathbb{F}_q . Its weighted cardinality is

$$(2.1) \quad \tilde{\#}I(a, q) := \sum_{E \in I(a, q)} \frac{1}{\#\text{Aut}(E)}.$$

A member of this isogeny class is ordinary if and only if $p \nmid a$; henceforth, we assume this is the case.

Fix an element $\gamma_0 \in G(\mathbb{Q})$ with characteristic polynomial

$$f_0(T) = f_{a,q}(T) := T^2 - aT + q.$$

Newton polygon considerations show that exactly one root of $f_{a,q}(T)$ is a p -adic unit, and in particular $f_{a,q}(T)$ has distinct roots. Therefore, γ_0 is regular semisimple. Moreover, any other element of $G(\mathbb{Q})$ with the same characteristic polynomial is conjugate to γ_0 .

Let $K = K_{a,q} = \mathbb{Q}[T]/f(T)$; it is a quadratic imaginary field. If $E \in I(a, q)$, then its endomorphism algebra is $\text{End}(E) \otimes \mathbb{Q} \cong K$. The centralizer G_{γ_0} of γ_0 in G is the restriction of scalars torus $G_{\gamma_0} \cong \mathbf{R}_{K/\mathbb{Q}}\mathbf{G}_m$.

If α is an invariant of an isogeny class, we will variously denote it as $\alpha(a, q)$, $\alpha(f_0)$, or $\alpha(\gamma_0)$, depending on the desired emphasis.

2.2. The Steinberg quotient. We review the general definition of the Steinberg quotient. Let G be a split, reductive group of rank r , with simply connected derived group G^{der} and Lie algebra \mathfrak{g} ; further assume that $G/G^{\text{der}} \cong \mathbf{G}_m$. (In the case of interest for this paper, $G = \text{GL}_2$, $r = 2$, and $G^{\text{der}} = \text{SL}_2$.)

Let T be a split maximal torus in G , $T^{\text{der}} = T \cap G^{\text{der}}$ (note that T^{der} is *not* the derived group of T), and let W be the Weyl group of G relative to T . Let $A^{\text{der}} = T^{\text{der}}/W$ be the Steinberg quotient for the semisimple group G^{der} . It is isomorphic to the affine space of dimension $r - 1$.

Let $A = A^{\text{der}} \times \mathbf{G}_m$ be the analogue of the Steinberg quotient for the reductive group G , cf [7]. We think of A as the space of “characteristic polynomials”. There is a canonical map

$$(2.2) \quad G \xrightarrow{\epsilon} A$$

Since $G/G^{\text{der}} \cong \mathbf{G}_m$, we have

$$A \cong \mathbb{A}^{r-1} \times \mathbf{G}_m \subset \mathbb{A}^r.$$

2.3. Gekeler numbers. We resume our discussion of elliptic curves, and let $G = \mathrm{GL}_2$. As in §2.1, fix data (a, q) defining an ordinary isogeny class over \mathbb{F}_q . Recall that, to each finite prime ℓ , Gekeler has assigned a local probability $\nu_\ell(a, q)$ (1.1)-(1.2). We give a geometric interpretation of this ratio, as follows.

Since G is a group scheme over \mathbb{Z} , for any finite prime ℓ , we have a well-defined group $G(\mathbb{Z}_\ell)$, which is a (hyper-special) maximal compact subgroup of $G(\mathbb{Q}_\ell)$, as well as the “truncated” groups $G(\mathbb{Z}_\ell/\ell^n)$ for every integer $n \geq 0$.

Recall that, given the fixed data (a, q) , we have chosen an element $\gamma_0 \in G(\mathbb{Q})$. Since the conjugacy class of a semisimple element of a general linear group is determined by its characteristic polynomial, γ_0 is well-defined up to conjugacy.

Let ℓ be any finite prime (we allow the possibility $\ell = p$); using the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_\ell$ we identify γ_0 with an element of $G(\mathbb{Q}_\ell)$. In fact, if $\ell \neq p$, then γ_0 is a regular semisimple element of $G(\mathbb{Z}_\ell)$.

For a fixed (notationally suppressed) positive integer n , the average value of $\#\mathfrak{c}^{-1}(a)$, as a ranges over $A(\mathbb{Z}_\ell/\ell^n)$, is

$$\#G(\mathbb{Z}_\ell/\ell^n)/\#A(\mathbb{Z}_\ell/\ell^n).$$

Consequently, we set

$$(2.3) \quad \nu_{\ell,n}(a, q) = \nu_{\ell,n}(\gamma_0) = \frac{\#\{\gamma \in G(\mathbb{Z}_\ell/\ell^n) : \gamma \sim (\gamma_0 \bmod \ell^n)\}}{\#G(\mathbb{Z}_\ell/\ell^n)/\#A(\mathbb{Z}_\ell/\ell^n)},$$

and rewrite (1.3) (and extend it to the case of \mathbb{F}_q) as

$$(2.4) \quad \nu_\ell(a, q) = \lim_{n \rightarrow \infty} \nu_{\ell,n}(a, q).$$

Here, we have exploited the fact that two semisimple elements of GL_2 are conjugate if and only if their characteristic polynomials are the same. Note that the denominator of (2.4) coincides with that of Gekeler’s definition [8, (3.7)]. Indeed,

$$(2.5) \quad \#G(\mathbb{Z}/\ell^n)/\#A(\mathbb{Z}/\ell^n) = \frac{\ell(\ell-1)(\ell^2-1)\ell^{4n-4}}{(\ell-1)\ell^{n-1}\ell^n} = (\ell^2-1)\ell^{2n-2}.$$

For $\ell = p$, γ_0 lies in $\mathrm{GL}_2(\mathbb{Q}_p) \cap \mathrm{Mat}_2(\mathbb{Z}_p)$. We make the apparently ad hoc definition

$$(2.6) \quad \nu_p(a, q) = \lim_{n \rightarrow \infty} \frac{\#\{\gamma \in \mathrm{Mat}_2(\mathbb{Z}_p/p^n) : \gamma \sim (\gamma_0 \bmod p^n)\}}{\#G(\mathbb{Z}_p/p^n)/\#A(\mathbb{Z}_p/p^n)},$$

where we have briefly used \sim to denote similarity of matrices under the action of $\mathrm{GL}_2(\mathbb{Z}_p/p^n)$. In the case where $q = p$, this recovers Gekeler’s definition (1.2).

Finally, we follow [8, (3.3)] and, inspired by the Sato-Tate measure, define an archimedean term

$$(2.7) \quad \nu_\infty(a, q) = \frac{2}{\pi} \sqrt{1 - \frac{a^2}{4q}}.$$

2.4. The Langlands and Kottwitz approach. For Shimura varieties of PEL type, Kottwitz proved [14] Langlands’s conjectural expression of the zeta function of that Shimura variety in terms of automorphic L-functions on the associated group. A key, albeit elementary, tool in this proof is the fact that the isogeny class of a (structured) abelian variety can be expressed in terms of an orbital integral. The special case where the Shimura variety in question is a modular curve, so that the abelian varieties are simply elliptic curves, has enjoyed several detailed presentations in the literature (e.g., [5], [19] and, to a lesser extent, [1]), and so we content ourselves here with the relevant statement.

As in §2.1, fix data (a, q) which determines an isogeny class of ordinary elliptic curves over \mathbb{F}_q , and let $\gamma_0 \in G(\mathbb{Q})$ be a suitable choice. If $E \in I(a, q)$, then for each $\ell \nmid q$ there is an isomorphism $H^1(E_{\mathbb{F}_q}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell^{\oplus 2}$ which takes the Frobenius endomorphism of E to γ_0 .

There is an additive operator F on $H_{\text{cris}}^1(E, \mathbb{Q}_q)$. It is σ -linear, in the sense that if $a \in \mathbb{Q}_q$ and $x \in H_{\text{cris}}^1(E, \mathbb{Q}_q)$, then $F(ax) = a^\sigma F(x)$. To F corresponds some $\delta_0 \in G(\mathbb{Q}_q)$, well-defined up to σ -conjugacy. (Recall that δ and δ' are σ -conjugate if there exists some $h \in G(\mathbb{Q}_q)$ such that $h^{-1}\delta h^\sigma = \delta'$.) The two elements are related by $N_{\mathbb{Q}_q/\mathbb{Q}_p}(\delta_0) \sim \gamma_0$.

Let G_{γ_0} be the centralizer of γ_0 in G . Let $G_{\delta_0\sigma}$ be the twisted centralizer of δ_0 in $G_{\mathbb{Q}_q}$; it is an algebraic group over \mathbb{Q}_p .

Finally, let \mathbb{A}_f^p denote the prime-to- p finite adeles, and let $\hat{\mathbb{Z}}_f^p \subset \mathbb{A}_f^p$ be the subring of everywhere-integral elements. With these notational preparations, we have

Proposition 2.1. *The weighted cardinality of an ordinary isogeny class of elliptic curves is given by*

$$(2.8) \quad \#I(a, q) = \text{vol}(G_{\gamma_0}(\mathbb{Q}) \backslash G_{\gamma_0}(\mathbb{A}_f)) \cdot \int_{G_{\gamma_0}(\mathbb{A}_f^p) \backslash G(\mathbb{A}_f^p)} \mathbf{1}_{G(\hat{\mathbb{Z}}_f^p)}(g^{-1}\gamma_0 g) dg \cdot \int_{G_{\delta_0\sigma}(\mathbb{Q}_p) \backslash G(\mathbb{Q}_q)} \mathbf{1}_{G(\mathbb{Z}_q)} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}_{G(\mathbb{Z}_q)} (h^{-1}\delta_0 h^\sigma) dh.$$

Here, each group $G(\mathbb{Q}_\ell)$ has been given the Haar measure which assigns volume one to $G(\mathbb{Z}_\ell)$ (this is the so-called *canonical measure*, see §3.1.2). The choice of nonzero Haar measure on the centralizer $G_\gamma(\mathbb{Q}_\ell)$ is irrelevant, as long as the same choice is made for the global volume computation. Similarly, in the second, twisted orbital integral, $G(\mathbb{Q}_q)$ is given the Haar measure which assigns volume one to $G(\mathbb{Z}_q)$. Since we shall need to be able to say something about the volume term later, we need to fix the measures on $G_{\gamma_0}(\mathbb{Q}_\ell)$ for every ℓ . We choose the canonical measures μ^{can} on both G and G_{γ_0} at every place. These measures are defined below in §3.1.2.

The idea behind Proposition 2.1 is straight-forward. (We defer to [5] for details.) Fix $E \in I(a, q)$ and $H^1(E_{\mathbb{F}_q}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell^{\oplus 2}$ as above. This singles out an integral structure $H^1(E_{\mathbb{F}_q}, \mathbb{Z}_\ell) \subseteq \mathbb{Q}_\ell^{\oplus 2}$. If E' is any other member of $I(a, q)$, then the prime-to- p part of an \mathbb{F}_q -rational isogeny induces $E \rightarrow E'$ gives a new integral structure $H^1(E'_{\mathbb{F}_q}, \mathbb{Z}_\ell)$ on $\mathbb{Q}_\ell^{\oplus 2}$. Similarly, p -power isogenies give rise to new integral structures on the crystalline cohomology $H_{\text{cris}}^1(E, \mathbb{Q}_q)$. In this way, $I(a, q)$ is identified with $K^\times \backslash Y^p \times Y_p$, where Y^p ranges among γ_0 -stable lattices in $Y^1(E_{\mathbb{F}_q}, \mathbb{A}^p)$, and Y_p ranges among lattices in $H_{\text{cris}}^1(E, \mathbb{Q}_q)$ stable under δ_0 and $p\delta_0^{-1}$. It is now straight-forward to use an orbital integral to calculate the automorphism-weighted, or groupoid, cardinality of the quotient set $K^\times \backslash Y^p \times Y_p$ (e.g., [11, §6]).

We remark that most expositions of Proposition 2.1 refer to a geometric context in which $\mathbf{1}_{G(\hat{\mathbb{Z}}_f^p)}$ is replaced with the characteristic function of an open compact subgroup which is sufficiently small that objects have trivial automorphism groups, so that the corresponding Shimura variety is a smooth and quasiprojective fine moduli space. However, this assumption is not necessary for the counting argument underlying (2.8); see, for instance, [5, 3(b)].

3. COMPARISON OF GEKELER NUMBERS WITH ORBITAL INTEGRALS

The calculation is based on the interplay between several G -invariant measures on the adjoint orbits in G . We start by carefully reviewing the definitions and the normalizations of all Haar measures involved.

3.1. Measures on groups and orbits. Let $\pi_n : \mathbb{Z}_\ell \rightarrow \mathbb{Z}_\ell / \ell^n$ be the truncation map. For any \mathbb{Z}_ℓ -scheme \mathcal{X} , we denote by $\pi_n^\mathcal{X}$ the corresponding map

$$\pi_n^\mathcal{X} : \mathcal{X}(\mathbb{Z}_\ell) \rightarrow \mathcal{X}(\mathbb{Z}_\ell / \ell^n)$$

induced by π_n .

Once and for all, fix the Haar measure on $\mathbb{A}^1(\mathbb{Q}_\ell)$ such that the volume of \mathbb{Z}_ℓ is 1. We will denote this measure by dx . The key observation that will play a role in our calculations is that with this normalization, the fibres of the standard projection $\pi_n^{\mathbb{A}^d} : \mathbb{A}^d(\mathbb{Z}_\ell) \rightarrow \mathbb{A}^d(\mathbb{Z}_\ell / \ell^n)$ have volume ℓ^{-nd} .

We also observe that there are two approaches to normalizing a Haar measure on the set of \mathbb{Q}_ℓ -points of an arbitrary algebraic group G : one can either fix a maximal compact subgroup and assign volume 1 to it; or one can fix a volume form ω_G on G with coefficients in \mathbb{Z} , and thus get the measure $|\omega_G|_\ell$ on each $G(\mathbb{Q}_\ell)$. Additionally, the measure that will be the most useful for us to study Gekeler-type ratios is the so-called Serre-Oesterlé measure (which turns out to be the measure that B. Gross calls *canonical* in [10], but which is different from, though closely related to, the measure that we call canonical here).

3.1.1. Serre-Oesterlé measure. Let \mathcal{X} be a smooth scheme over \mathbb{Z}_ℓ . Then there is the so-called Serre-Oesterlé measure on X , which we will denote by μ_X^{SO} . It is defined in [20, §3.3], see also [21] for an attractive equivalent definition. For a smooth scheme that has a non-vanishing gauge form this definition coincides with the definition of A. Weil [22], and by [22, Theorem 2.2.5] (extended by Batyrev [3, Theorem 2.7]), this measure has the property that $\text{vol}^{\text{SO}}(\mathcal{X}(\mathbb{Z}_\ell)) = \#\mathcal{X}(\mathbb{F}_\ell) \ell^{-d}$, where d is the dimension of the generic fiber of \mathcal{X} . In particular, $\mu_{\mathbb{A}^1}^{\text{SO}}$ is the Haar measure on the affine line such that $\text{vol}^{\text{SO}}(\mathbb{A}^1(\mathbb{Z}_\ell)) = \ell \ell^{-1} = 1$, i.e., $\mu_{\mathbb{A}^1(\mathbb{Q}_\ell)}^{\text{SO}}$ coincides with $|dx|_\ell$. Similarly, on any d -dimensional affine space \mathbb{A}^d , the Serre-Oesterlé measure gives $\mathbb{A}^d(\mathbb{Z}_\ell)$ volume 1.

The algebraic group GL_2 is a smooth group scheme defined over \mathbb{Z} ; in particular, for every ℓ , $\text{GL}_2 \times_{\mathbb{Z}} \mathbb{Z}_\ell$ is a smooth scheme over \mathbb{Z}_ℓ , so μ^{SO} gives $\text{GL}_2(\mathbb{Z}_\ell)$ volume

$$\mu^{\text{SO}}(\text{GL}_2(\mathbb{Z}_\ell)) = \frac{\#\text{GL}_2(\mathbb{F}_\ell)}{\ell^d} = \frac{\ell(\ell-1)(\ell^2-1)}{\ell^4}.$$

3.1.2. The canonical measures. Let G be a reductive group over \mathbb{Q}_ℓ ; then Gross [10, Sec. 4] constructs a canonical volume form ω_G , which does not vanish on the special fibre of the canonical model \underline{G} over \mathbb{Z}_ℓ . If G is unramified over \mathbb{Q}_ℓ , then ω_G recovers the Serre-Oesterlé measure, insofar as

$$\int_{\underline{G}(\mathbb{Z}_\ell)} |\omega_G|_\ell = \frac{\#\underline{G}^\kappa(\mathbb{F}_\ell)}{\ell^{\dim G}},$$

where \underline{G}^κ is the closed fibre of \underline{G} [10, Prop. 4.7].

The measure most commonly used in the calculation of orbital integrals, traditionally denoted by μ^{can} , is closely related to $|\omega_G|$. By definition, μ^{can} is normalized by giving volume 1 to the canonical compact subgroup $\underline{G}(\mathbb{Z}_\ell)$. For an unramified group G , this is a hyperspecial maximal compact subgroup $\underline{G}(\mathbb{Z}_\ell)$. Thus, for $G = \text{GL}_2$, we have: $\mu^{\text{can}}(G(\mathbb{Z}_\ell)) = 1$.

We will also need to understand the canonical measures for tori in G , which arise as the centralizers of semisimple elements. For a torus T , by definition, $\mu_T^{\text{can}}(\underline{T}^\circ(\mathbb{Z}_\ell)) = 1$, where \underline{T}° is the connected component of the canonical integral model for T (which will be discussed in more detail in §4.1 below).

3.1.3. *The geometric measure.* We will use a certain quotient measure μ^{geom} on the orbits, which is called the geometric measure in [7]. This measure is defined using the Steinberg map \mathfrak{c} (2.2); we return to the setting of §2.2.

For a general reductive group G and $\gamma \in G(\mathbb{Q}_\ell)$ regular semisimple, the fibre over $\mathfrak{c}(\gamma)$ is the stable orbit of γ , which is a finite union of rational orbits. In our setting with $G = \text{GL}_2$, the fibre $\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))$ is a single rational orbit, which substantially simplifies the situation. From here onwards, we work only with $G = \text{GL}_2$.

Consider the measure given by the form ω_G on G , and the measure on $A = \mathbb{A}^1 \times \mathbb{G}_m$ which is the product of the measures associated with the form dt on \mathbb{A}^1 and ds/s on \mathbb{G}_m , where we denote the coordinates on A by (t, s) . We will denote this measure by $|d\omega_A|$.

The form ω_G is a generator of the top exterior power of the cotangent bundle of G . For each orbit $\mathfrak{c}^{-1}(t, s)$ (note that such an orbit is a variety) there is a unique generator $\omega_{\mathfrak{c}(\gamma)}^{\text{geom}}$ of the top exterior power of the cotangent bundle on the orbit $\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))$ such that

$$\omega_G = \omega_{\mathfrak{c}(\gamma)}^{\text{geom}} \wedge \omega_A.$$

Then for any $\phi \in C_c^\infty(G(\mathbb{Q}_\ell))$,

$$\int_{G(\mathbb{Q}_\ell)} \phi(g) d|\omega_G| = \int_{A(\mathbb{Q}_\ell)} \int_{\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))} \phi(g) d|\omega_{\mathfrak{c}(\gamma)}^{\text{geom}}| |d\omega_A(t, s)|.$$

This measure also appears in [7], and it is discussed in detail in §4 below.

3.1.4. *Orbital integrals.* There are two kinds of orbital integrals that will be relevant for us; they differ only in the normalization of measures on the orbits. Let γ be a regular semisimple element of $G(\mathbb{Q}_\ell)$, and let ϕ be a locally constant compactly supported function on $G(\mathbb{Q}_\ell)$. Let T be the centralizer G_γ of γ . Since γ is regular (i.e., the roots of the characteristic polynomial of γ are distinct) and semisimple, T is a maximal torus in G .

First, we consider the orbital integral with respect to the geometric measure:

Definition 3.1. Define $O_\gamma^{\text{geom}}(\phi)$ by

$$O_\gamma^{\text{geom}}(\phi) := \int_{T(\mathbb{Q}_\ell) \backslash G(\mathbb{Q}_\ell)} \phi(g^{-1}\gamma g) d\mu_\gamma^{\text{geom}},$$

where μ_γ^{geom} is the measure on the orbit of γ associated with the corresponding differential form $\omega_{\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))}^{\text{geom}}$ as in §3.1.3 above.

Second, there is the canonical orbital integral over the orbit of γ , defined as follows. The orbit of γ can be identified with the quotient $T(\mathbb{Q}_\ell) \backslash G(\mathbb{Q}_\ell)$. Both $T(\mathbb{Q}_\ell)$ and $G(\mathbb{Q}_\ell)$ are endowed with canonical measures, as above in §3.1.2. Then there is unique quotient measure on $T(\mathbb{Q}_\ell) \backslash G(\mathbb{Q}_\ell)$, which will be denoted $d\mu_\gamma^{\text{can}}$. The canonical orbital integral will be the integral with respect to this measure on the orbit (also considered as a distribution on the space of locally constant compactly supported functions on $G(\mathbb{Q}_\ell)$):

Definition 3.2. Define $O_\gamma^{\text{can}}(\phi)$ by

$$O_\gamma^{\text{can}}(\phi) := \int_{T(\mathbb{Q}_\ell) \backslash G(\mathbb{Q}_\ell)} \phi(g^{-1}\gamma g) d\mu_\gamma^{\text{can}}.$$

By definition, the distributions O_γ^{geom} and O_γ^{can} differ by a multiple that is a function of γ . This ratio (which we feel should probably be well-known but was hard to find in the literature, see also [7]) is computed in §4 below.

We will first relate Gekeler's ratios to orbital integrals with respect to the geometric measure, in a natural way, and from there will get the relationship with the canonical orbital integrals, which are more convenient to use for the purposes of computing the global volume term appearing in the formula of Langlands and Kottwitz.

3.2. Gekeler numbers and volumes, for ℓ not equal to p . From now on, $G = \text{GL}_2$, $\gamma_0 = \gamma_{a,q}$, and ℓ is a fixed prime distinct from p . Our first goal is to relate the Gekeler number $\nu_\ell(a, q)$ (2.4) to an orbital integral $O_{\gamma_0}^{\text{geom}}(\phi_0)$ of a suitable test function ϕ_0 with respect to $d\left|\omega_{\mathfrak{c}(\gamma)}^{\text{geom}}\right|$. (Recall that γ_0 is the element of $G(\mathbb{Q}_\ell)$ determined by E , and in this case since $\ell \neq p$, it lies in $G(\mathbb{Z}_\ell)$.) In order to do this we define natural subsets of $G(\mathbb{Q}_\ell)$ whose volumes are responsible for this relationship.

Recall (2.3) the definition of $\nu_{\ell,n}(\gamma_0)$. For each positive integer n , consider the subset V_n of $\text{GL}_2(\mathbb{Z}_\ell)$ defined as

$$(3.1) \quad V_n = V_n(\gamma_0) := \{\gamma \in \text{GL}_2(\mathbb{Z}_\ell) \mid f_\gamma(T) \equiv f_0(T) \pmod{\ell^n}\}$$

$$(3.2) \quad = \left\{ \gamma \in \text{GL}_2(\mathbb{Z}_\ell) \mid \pi_n^A(\mathfrak{c}(\gamma)) = \pi_n^A(\mathfrak{c}(\gamma_0)) \right\}.$$

and set

$$(3.3) \quad V(\gamma_0) := \bigcap_{n \geq 1} V_n(\gamma_0).$$

We define an auxiliary ratio:

$$(3.4) \quad v_n(\gamma_0) := \frac{\text{vol}_{\mu_{\text{GL}_2}^{\text{SO}}}(V_n(\gamma_0))}{\ell^{-2n}}.$$

Now we would like to relate the limit of these ratios $v_n(\gamma_0)$ both to the limit of Gekeler ratios $\nu_{\ell,n}(\gamma_0)$ and to an orbital integral.

Let $\phi_0 = \mathbf{1}_{\text{GL}_2(\mathbb{Z}_\ell)}$ be the characteristic function of the maximal compact subgroup $\text{GL}_2(\mathbb{Z}_\ell)$ in $\text{GL}_2(\mathbb{Q}_\ell)$.

Proposition 3.3. *We have*

$$\lim_{n \rightarrow \infty} v_n(\gamma_0) = O_{\gamma_0}^{\text{geom}}(\phi_0).$$

Proof. Because equality of characteristic polynomials is equivalent to conjugacy in $\text{GL}_2(\mathbb{Q}_\ell)$, $V(\gamma_0)$ is the intersection of $\text{GL}_2(\mathbb{Z}_\ell)$ with the orbit $\mathcal{O}(\gamma_0)$ of γ_0 in $G = \text{GL}_2(\mathbb{Q}_\ell)$. Then the orbital integral $O_{\gamma_0}^{\text{geom}}(\phi_0)$ is nothing but the volume of the set $V(\gamma_0)$, as a subset of $\mathcal{O}(\gamma_0)$, with respect to the measure $d\mu_{\gamma_0}^{\text{geom}}$.

Let $a_0 = \mathfrak{c}(\gamma_0) = (a, q) \in \mathbb{A}^1 \times \mathbb{G}_m(\mathbb{Q}_\ell)$, and let $U_n(a_0)$ be its $\ell^{-n} \times \ell^{-n}$ -neighborhood. Its Serre-Oesterle volume is $\text{vol}_{\mu_A^{\text{SO}}}(U_n(\gamma_0)) = \ell^{-2n}$.

Moreover, $V_n(\gamma_0) = \mathfrak{c}^{-1}(U_n(\gamma_0)) \cap \text{GL}_2(\mathbb{Z}_\ell)$. Consequently,

$$(3.5) \quad \begin{aligned} \lim_{n \rightarrow \infty} v_n(\gamma_0) &= \lim_{n \rightarrow \infty} \frac{\text{vol}_{\mu_{\text{GL}_2}^{\text{SO}}}(\mathfrak{c}^{-1}(U_n(\gamma_0)) \cap \text{GL}_2(\mathbb{Z}_\ell))}{\text{vol}_{\mu_A^{\text{SO}}}(U_n(\gamma_0))} \\ &= \lim_{n \rightarrow \infty} \frac{\text{vol}_{|d\omega_G|}(\mathfrak{c}^{-1}(U_n(\gamma_0)) \cap \text{GL}_2(\mathbb{Z}_\ell))}{\text{vol}_{|d\omega_A|}(U_n(\gamma_0))} = \text{vol}_{\mu_{\gamma_0}^{\text{geom}}}(V(\gamma_0)), \end{aligned}$$

by definition of the geometric measure. \square

Next, let us relate the ratios v_n to the Gekeler ratios.

Proposition 3.4. *We have the relation*

$$\lim_{n \rightarrow \infty} v_n(\gamma_0) = \frac{\#\mathrm{SL}_2(\mathbb{F}_\ell)}{\ell^3} \lim_{n \rightarrow \infty} v_{\ell,n}(\gamma_0) = \frac{\ell^2 - 1}{\ell^2} v_\ell(a, q).$$

Proof. Let $\pi_n = \pi_n^{\mathrm{GL}_2} : \mathrm{GL}_2(\mathbb{Z}_\ell) \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n)$. To ease notation slightly, let $V_n = V_n(\gamma_0)$. Let $S_n \subset \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the set that appears in the numerator (2.3):

$$S_n := \{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^n) \mid f_\gamma(T) \equiv f_0(T) \pmod{\ell^n}\}.$$

We claim that, for large enough n (depending on the discriminant of f), the following hold:

- (i) $V_n = \pi_n^{-1}(S_n)$ and $\pi_n|_{V_n} : V_n \rightarrow S_n$ is surjective;
- (ii) We have the equality

$$(3.6) \quad \mathrm{vol}_{\mu_{\mathrm{GL}_2}^{\mathrm{SO}}}(V_n) = \ell^{-4n} \#S_n.$$

The first claim is needed to establish the second one; and provided the second claim holds, we get (where the denominator of Gekeler's ratio is handled as in (2.5) above):

$$(3.7) \quad v_n(\gamma_0) = \frac{\ell^{-4n} \#S_n}{\ell^{-2n}} = \frac{\#S_n}{\ell^{2n}} = \frac{\#S_n \#\mathrm{SL}_2(\mathbb{F}_\ell)}{\#\mathrm{SL}_2(\mathbb{F}_\ell) \ell^{3(n-1)} \ell^{-n} \ell^3} = \frac{\#\mathrm{SL}_2(\mathbb{F}_\ell)}{\ell^3} v_{\ell,n}(\gamma_0),$$

as required. Thus, it remains to verify the two claims.

(i). Taking characteristic polynomials commutes with reduction mod ℓ^n , since the coefficients of the characteristic polynomial are themselves polynomial in the matrix entries of γ , and reduction mod ℓ^n is a ring homomorphism. Thus, $\pi_n^{-1}(S_n) = V_n$. Since GL_2 is a smooth scheme over \mathbb{Z}_ℓ , π_n is surjective for all n .

(ii) Since GL_2 is smooth over the residue field \mathbb{F}_ℓ , all fibres of π_n have volume equal to ℓ^{-4n} . By part (i), the set V_n is a disjoint union of fibres of π_n , and the number of these fibres is $\#\pi_n(V_n) = \#S_n$. Thus, the volume of V_n is exactly ℓ^{-4n} times the number of points in the image of the set in the numerator under this projection. \square

Combining Propositions 3.3 and 3.4, we immediately obtain:

Corollary 3.5. *The Gekeler numbers relate to orbital integrals via*

$$v_\ell(a, q) = \frac{\ell^3}{\#\mathrm{SL}_2(\mathbb{F}_\ell)} O_{\gamma_0}^{\mathrm{geom}}(\phi_0).$$

3.3. $\ell = p$ revisited. We now consider $v_p(a, q)$ in a similar light. Since $\det(\gamma_0) = q$, γ_0 lies in $\mathrm{Mat}_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p)$ but *not* in $\mathrm{GL}_2(\mathbb{Z}_p)$, and we must consequently modify the argument of §3.2.

For integers m and n , let $\lambda_{m,n} = \begin{pmatrix} p^m & 0 \\ 0 & p^n \end{pmatrix}$, and let $C_{m,n} = \mathrm{GL}_2(\mathbb{Z}_p) \lambda_{m,n} \mathrm{GL}_2(\mathbb{Z}_p)$. The Cartan decomposition for GL_2 asserts that $\mathrm{GL}_2(\mathbb{Q}_p)$ is the disjoint union

$$\mathrm{GL}_2(\mathbb{Q}_p) = \bigcup_{m \geq n} C_{m,n},$$

so that

$$\mathrm{Mat}_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p) = \bigcup_{0 \leq n \leq m} C_{m,n}.$$

We now express $\nu_p(a, q)$ as an orbital integral. Recall that $q = p^e$. Since we consider an ordinary isogeny class, the element $\gamma_0 \in \mathrm{GL}_2(\mathbb{Q}_p)$ actually can be chosen to have the form $\gamma_0 = \begin{pmatrix} u_1 p^e & 0 \\ 0 & u_2 \end{pmatrix}$, where $u_1, u_2 \in \mathbb{Z}_p$ are units, and thus in particular, $\gamma_0 \in C_{e,0}$.

Lemma 3.6. *Let ϕ_q be the characteristic function of $C_{e,0} = \mathrm{GL}_2(\mathbb{Z}_p) \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_p)$. Then*

$$\nu_p(a, q) = \frac{p^3}{\#\mathrm{SL}_2(\mathbb{F}_p)} O_{\gamma_0}^{\mathrm{geom}}(\phi_q).$$

Proof. The proof is similar to the case $\ell \neq p$, with one key modification. There, we are using the reduction mod ℓ^n map π_n defined on $G(\mathbb{Z}_\ell)$. Here, we need to extend the map π_n to a set that contains γ_0 .

Let $\pi_n^M : \mathrm{Mat}_2(\mathbb{Z}_p) \rightarrow \mathrm{Mat}_2(\mathbb{Z}_p/p^n)$ be the projection map, and let $\mathfrak{c} : \mathrm{GL}_2(\mathbb{Q}_p) \rightarrow A(\mathbb{Q}_p)$ be the characteristic polynomial map. As in §3.2 above, we define the sets

$$\begin{aligned} U_n &:= \{a = (a_0, a_1) \in A(\mathbb{Z}_p) \mid a_i \equiv a_i(\gamma_0) \pmod{p^n}, i = 0, 1\} \\ S_n &:= \{\gamma \in \mathrm{Mat}_2(\mathbb{Z}_p/p^n) : \gamma \sim \pi_n^M(\gamma_0)\} \\ V_n &:= (\pi_n^M)^{-1}(S_n) \subset \mathrm{Mat}_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p). \end{aligned}$$

As before, informally, we think of U_n as a neighbourhood of the point given by the coefficients of the characteristic polynomial of γ_0 in the Steinberg-Hitchin base, and we think of V_n as the intersection of the corresponding neighbourhood of the orbit of γ_0 in $\mathrm{GL}_2(\mathbb{Q}_p)$ with $\mathrm{Mat}_2(\mathbb{Z}_p)$. In the case $\ell \neq p$ we had $\mathrm{GL}_2(\mathbb{Z}_\ell)$ in the place of $\mathrm{Mat}_2(\mathbb{Z}_p)$ in this description, and so it was clear that the evaluation of the volume of V_n would lead to the orbital integral of ϕ_0 , the characteristic function of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Here, we need to make the connection between the set V_n and our function ϕ_q .

We claim that if $n > e$, then $V_n \subset C_{e,0}$. Indeed, suppose $\gamma \in V_n$. Then, since the characteristic polynomial of γ is congruent to that of γ_0 , the trace of γ is a p -adic unit. Then γ cannot lie in any double coset $C_{m,n}$ with both m, n positive, because if it did, its trace would have been divisible by $p^{\min(m,n)}$. Then γ has to lie in a double coset of the form $C_{e+m,-m}$ for some $m \geq 0$; but if $m > 0$, then such a double coset has empty intersection with $\mathrm{Mat}_2(\mathbb{Z}_p)$, so $m = 0$ and the claim is proved.

As in the proof of Proposition 3.4 (iii), the volume of the set V_n equals $p^{-4n} \#S_n$. The rest of the proof repeats the proofs of Proposition 3.4 and Corollary 3.5. We again set $V(\gamma_0) = \bigcap_{n \geq 1} V_n \subset C_{e,0}$. Since π_n^M is surjective, $V(\gamma_0) = O(\gamma_0) \cap C_{e,0}$. By (3.5),

$$O_{\gamma_0}^{\mathrm{geom}}(\phi_q) = \lim_{n \rightarrow \infty} \frac{\mathrm{vol}_{\mu_{\mathrm{GL}_2}^{\mathrm{SO}}} V_n(\gamma_0)}{\mathrm{vol}_{\mu_A^{\mathrm{SO}}}(U_n)} = \lim_{n \rightarrow \infty} \frac{\#S_n(\gamma_0) p^{-4n}}{p^{-2n}},$$

and the statement follows by (3.7), which does not require any modification. □

Recall that, in terms of the data (a, q) , we have also computed a representative δ_0 for a σ -conjugacy class in $\mathrm{GL}_2(\mathbb{Q}_q)$. It is characterized by the fact that, possibly after adjusting γ_0 in its conjugacy class, we have $N_{\mathbb{Q}_q/\mathbb{Q}_p}(\delta_0) = \gamma_0$.

The twisted centralizer $G_{\delta_0\sigma}$ of δ_0 is an inner form of the centralizer G_{γ_0} [13, Lemma 5.8]; since γ_0 is regular semisimple, G_{γ_0} is a torus, and thus $G_{\delta_0\sigma}$ is isomorphic to G_{γ_0} . Using this, any choice of Haar measure on $G_{\delta_0\sigma}(\mathbb{Q}_p)$ induces one on $G_{\gamma_0}(\mathbb{Q}_p)$.

If ϕ is a function on $G(\mathbb{Q}_q)$, denote its twisted (canonical) orbital integral along the orbit of δ_0 by

$$TO_{\delta_0}^{\text{can}}(\phi) = \int_{G_{\delta_0\sigma}(\mathbb{Q}_p) \backslash G(\mathbb{Q}_q)} \phi(h^{-1}\delta_0 h^\sigma) d\mu^{\text{can}}.$$

Lemma 3.7. *Let $\phi_{p,q}$ be the characteristic function of $\text{GL}_2(\mathbb{Z}_q)\lambda_{0,1}\text{GL}_2(\mathbb{Z}_q)$. Then*

$$TO_{\delta_0}^{\text{can}}(\phi_{p,q}) = O_{\gamma_0}^{\text{can}}(\phi_q).$$

Proof. The asserted matching of twisted orbital integrals on $\text{GL}_2(\mathbb{Q}_q)$ with orbital integrals on $\text{GL}_2(\mathbb{Q}_p)$ is one of the earliest known instances of the fundamental lemma ([16]; see also [18, Sec. 4], [9, (E.4.9)] or even [1, Sec. 2.1]). Indeed, the base change homomorphism of the Hecke algebras matches the characteristic function of $\text{GL}_2(\mathbb{Z}_q)\lambda_{1,0}\text{GL}_2(\mathbb{Z}_q)$ with $\phi_q + \phi$, where ϕ is a linear combination of the characteristic functions of $C_{a,b}$ with $a + b = e$ and $a, b > 0$. As shown in the proof of the previous lemma, the orbit of γ_0 does not intersect the double cosets $C_{a,b}$ with $a, b > 0$, and thus the only non-zero term on the right-hand side is $O_{\gamma_0}^{\text{can}}(\phi_q)$. \square

4. CANONICAL MEASURE VS. GEOMETRIC MEASURE

Finally, we need to relate the orbital integral with respect to the geometric measure as above to the canonical orbital integrals. A very similar calculation is discussed in [7] (and as the authors point out, surprisingly, it seemed impossible to find in earlier literature). Since our normalization of local measures seems to differ by an interesting constant from that of [7] at ramified finite primes, we carry out this calculation in our special case.

4.1. Canonical measure and L -functions. Here we briefly review the facts that go back to the work of Weil, Langlands, Ono, Gross, and many others, that show the relationship between convergence factors that can be used for Tamagawa measures and various Artin L -functions. Our goal is to introduce the Artin L -factors that naturally appear in the computation of the canonical measures. To any reductive group G over \mathbb{Q}_ℓ , Gross attaches a motive $M = M_G$ [10]; following his notation, we consider $M^\vee(1)$ – the Tate twist of the dual of M . For any motive M we let $L_\ell(s, M)$ be the associated local Artin L -function. We will write $L_\ell(M)$ for the value of $L_\ell(s, M)$ at $s = 0$. The value $L_\ell(M^\vee(1))$ is always a positive rational number, related to the canonical measure reviewed in §3.1.2. In particular, if G is quasi-split over \mathbb{Q}_ℓ , then

$$(4.1) \quad \mu_G^{\text{can}} = L_\ell(M^\vee(1))|\omega_G|_\ell$$

([10, 4.7 and 5.1]).

We shall also need a similar relation between volumes and Artin L -functions in the case when $G = T$ is an algebraic torus which is not necessarily anisotropic. Here we follow [4]. Suppose that T splits over a finite Galois extension L of \mathbb{Q}_ℓ ; let κ_L be the residue field of L , and let I be the inertia subgroup of the Galois group $\text{Gal}(L/\mathbb{Q}_\ell)$. Let $X^*(T)$ be the group of rational characters of T . Let \mathcal{T} be the Néron model of T over \mathbb{Z}_ℓ , with the connected component of the identity denoted by \mathcal{T}° . This is the canonical model for T referred to in 3.1.2.

Let Fr_L be the Frobenius element of $\text{Gal}(\kappa_L/\mathbb{F}_\ell)$. The Galois group of the maximal unramified sub-extension of L , which is isomorphic to $\text{Gal}(\kappa_L/\mathbb{F}_\ell)$, acts naturally on the I -invariants $X^*(T)^I$, giving rise to a representation which we will denote by ξ_T (and which is denoted by h in [4]),

$$\xi_T : \text{Gal}(\kappa_L/\mathbb{F}_\ell) \rightarrow \text{Aut}(X^*(T)^I) \simeq \text{GL}_{d_I}(\mathbb{Z}),$$

where $d_I = \text{rank}(X^*(T)^I)$. Then the associated local Artin L -factor is defined as:

$$L_\ell(s, \xi_T) := \det \left(1_{d_I} - \frac{\xi_T(\text{Fr}_L)}{\ell^s} \right)^{-1}.$$

Proposition 4.1. ([4, Proposition 2.14])

$$L_\ell(1, \xi_T)^{-1} = \# \mathcal{T}^\circ(\mathbb{F}_\ell) \ell^{-\dim(T)} = \int_{\mathcal{T}^\circ(Z_\ell)} |\omega_T|_\ell.$$

We observe that by definition [10, §4.3], since $G = T$ is an algebraic torus, the canonical parahoric \underline{T}° is \mathcal{T}° ; the canonical volume form ω_T is the same as the volume form denoted by ω_p in [4].

We also note that the motive of the torus T is the Artin motive $M = X^*(T) \otimes \mathbb{Q}$. If T is anisotropic over \mathbb{Q}_ℓ , by the formula (6.6) (cf. also (6.11)) in [10], we have

$$L_\ell(M^\vee(1)) = L_\ell(1, \xi_T).$$

As in the first paragraph of §3.1.3, let G be a reductive group over \mathbb{Q}_ℓ with simply connected derived group G^{der} and connected center Z , and assume that $G/G^{\text{der}} \cong \mathbb{G}_m$.

Lemma 4.2. *Let $T \subset G$ be a maximal torus; let $T^{\text{der}} = T \cap G^{\text{der}}$. Then*

$$(4.2) \quad \frac{L_\ell(M_G^\vee(1))}{L_\ell(1, \xi_T)} = \frac{L_\ell(M_{G^{\text{der}}}^\vee(1))}{L_\ell(1, \xi_{T^{\text{der}}})}.$$

Proof. The motive M_H of a reductive group H , and thus $L_\ell(M_H^\vee(1))$, depends on H only up to isogeny [10, Lemma 2.1]. Since G is isogenous to $Z \times G^{\text{der}}$,

$$L_\ell(M_G^\vee(1)) = L_\ell(M_Z^\vee(1)) L_\ell(M_{G^{\text{der}}}^\vee(1)).$$

Because $G^{\text{der}} \cap Z$ is finite [7, (3.1)], so is $T^{\text{der}} \cap Z$. Therefore, the natural map $T^{\text{der}} \rightarrow T/Z$ is an isogeny onto its image. For dimension reasons it is an actual isogeny, and induces an isomorphism $X^*(T^{\text{der}}) \otimes \mathbb{Q} \cong X^*(T/Z) \otimes \mathbb{Q}$ of $\text{Gal}(\mathbb{Q}_\ell)$ -modules. Therefore, $L(s, \xi_{T^{\text{der}}}) = L(s, \xi_{T/Z})$, and thus

$$L(s, \xi_T) = L(s, \xi_{T/Z}) L(s, \xi_Z) = L(s, \xi_{T^{\text{der}}}) L(s, \xi_Z).$$

Identity (4.2) is now immediate. □

4.2. Weyl discriminants and measures. Our next immediate goal is to find an explicit constant $d(\gamma)$ such that $\mu_\gamma^{\text{can}} = d(\gamma) \mu_\gamma^{\text{geom}}$. We note that a similar calculation is carried out in [7]. However, the notation there is slightly different, and the key proof in [7] only appears for the field of complex numbers; hence, we decided to include this calculation here.

Let G be a split reductive group over \mathbb{Q}_ℓ ; choose a split maximal torus and associated root system R and set of positive roots R^+ .

Definition 4.3. *Let $\gamma \in G(\mathbb{Q}_\ell)$, let T be the centralizer of γ , and \mathfrak{t} the Lie algebra of T . Then the discriminant of γ is*

$$D(\gamma) = \prod_{\alpha \in R} (1 - \alpha(\gamma)) = \det(I - \text{Ad}(\gamma^{-1}))|_{\mathfrak{g}/\mathfrak{t}}.$$

4.2.1. *Weyl integration formula, revisited.* As pointed out in [7] (the paragraph above equation (3.28)), since both μ_γ^{can} and μ_γ^{geom} are invariant under the center, it suffices to consider the case $G = G^{\text{der}}$. So for the moment, let us assume that the group G is semisimple and simply connected; let $\phi \in C_c^\infty(\mathbb{Q}_\ell)$.

On one hand, the Weyl integration formula (we write a group-theoretic version of the formulation for the Lie algebra in [15, §7.7]) asserts that

$$(4.3) \quad \int_{G(\mathbb{Q}_\ell)} \phi(g) |d\omega_G| = \sum_T \frac{1}{|W_T|} \int_{T(\mathbb{Q}_\ell)} |D(\gamma)| \int_{T(\mathbb{Q}_\ell) \backslash G(\mathbb{Q}_\ell)} \phi(g^{-1}\gamma g) d|\omega_{T \backslash G}| d|\omega_T|,$$

by our definition of the measure $d|\omega_{T \backslash G}|$. (Here, the sum ranges over a set of representatives for $G(\mathbb{Q}_\ell)$ -conjugacy classes of maximal \mathbb{Q}_ℓ -rational tori in G , and W_T is the finite group $W_T = N_G(T)(\mathbb{Q}_\ell)/T(\mathbb{Q}_\ell)$.)

On the other hand we have, by definition of the geometric measure,

$$\int_{G(\mathbb{Q}_\ell)} \phi(g) d|\omega_G| = \int_{A(\mathbb{Q}_\ell)} \int_{\mathfrak{c}^{-1}(a)} \phi(g) d|\omega_\gamma^{\text{geom}}(g)| d\omega_A.$$

To compare the two measures, we need to match the integration over $A(\mathbb{Q}_\ell)$ with the sum of integrals over tori.

Up to a set of measure zero, $A(\mathbb{Q}_\ell)$ is a disjoint union of images of $T(\mathbb{Q}_\ell)$, as T ranges over the same set as in (4.3); and for each such T , the restriction of \mathfrak{c} to T is $|W_T|$ -to-one.

It remains to compute the Jacobian of this map for a given T . Over the algebraic closure of \mathbb{Q}_ℓ this calculation is done, for example, in [15, §14]; over \mathbb{Q}_ℓ , this only applies to the split torus T^{spl} . The answer over the algebraic closure is $c_T \prod_{\alpha > 0} (\alpha(x) - 1)$, where $c_T \in \bar{F}^\times$ is a constant (which depends on the torus T). We compute $|c_T|_\ell$ in the special case where T comes from a restriction of scalars in GL_2 .

Lemma 4.4. *Let T be a torus in $\text{GL}_2(\mathbb{Q}_\ell)$, and let c_T be the constant defined above. Then $|c_T|_\ell = 1$ if T is split or splits over an unramified extension, and $|c_T| = \ell^{-1/2}$ if T splits over a ramified quadratic extension. In particular, if $\gamma_0 \in \text{GL}_2(\mathbb{Q})$ and $T = \mathbf{R}_{K/\mathbb{Q}} \mathbf{G}_m$ is the centralizer of γ_0 as in §2.1, then $|c_T| = |\Delta_K|_\ell^{-1/2}$.*

Proof. We prove the lemma by direct calculation for GL_2 . First, let us compute $|c_T|$ for the split torus. Here we can just compute the Jacobian of the map $T^{\text{der}} \rightarrow T^{\text{der}}/W$ by hand. Since we are working with invariant differential forms, we can just do the Jacobian calculation on the Lie algebra; it suffices to compute the Jacobian of the map from \mathfrak{t} to \mathfrak{t}/W . Choose coordinates on the split torus in $\text{SL}_2 = \text{GL}_2^{\text{der}}$, so that elements of \mathfrak{t} are diagonal matrices with entries $(t, -t)$; then the canonical measure on \mathfrak{t} is nothing but dt . Now, the coordinate on \mathfrak{t}/W is $y = -t^2$; the form $\omega_{\mathbb{A}^1}$ is dx . The Jacobian of the change of variables from \mathfrak{t}/W to \mathbb{A}^1 is $-2t$. Thus, for the split torus $c = -1$: note that $2t$ is the product of positive roots (on the Lie algebra). Thus, $|c_T| = 1$.

Now, consider a general maximal torus T in GL_2 . Let T^{spl} be a split maximal torus; we have shown that $|c_{T^{\text{spl}}}| = 1$. The torus T is conjugate to T^{spl} over a quadratic field extension L . Let us briefly denote this conjugation map by ψ . Then the map $\mathfrak{c}|_T$ can be thought of as the conjugation $\psi : T \rightarrow T^{\text{spl}}$ (defined over L) followed by the map $\mathfrak{c}|_{T^{\text{spl}}}$. Then

$$c_T = c_{T^{\text{spl}}} \frac{\omega_T}{\psi^*(\omega_{T^{\text{spl}}})},$$

where $\psi^*(\omega_{T^{\text{spl}}})$ is the pullback of the canonical volume form on T^{spl} under ψ and the ratio $\frac{\omega_T}{\psi^*(\omega_{T^{\text{spl}}})}$ is a constant in L . We thus have

$$(4.4) \quad c_T = \left| \frac{\omega_T}{\psi^*(\omega_{T^{\text{spl}}})} \right|_L,$$

where $|\cdot|_L$ is the unique extension of the absolute value on \mathbb{Q}_ℓ to L .

At this point this is just a question about two tori, no longer requiring Steinberg section, and so we pass back to working with the group GL_2 rather than SL_2 . Now T is obtained by restriction of scalars from \mathbb{G}_m , and so we can compute $\psi^*(\omega_{T^{\text{spl}}})$ by hand. By definition, $T = \mathbf{R}_{L/\mathbb{Q}_\ell} \mathbb{G}_m$; $T^{\text{spl}} = \mathbb{G}_m \times \mathbb{G}_m$. The form $\omega_{T^{\text{spl}}}$ is

$$\omega_{T^{\text{spl}}} = \frac{du}{u} \wedge \frac{dv}{v},$$

where we denote the coordinates on $\mathbb{G}_m \times \mathbb{G}_m$ by (u, v) . Let $L = \mathbb{Q}_\ell(\sqrt{\epsilon})$, where ϵ is a non-square in \mathbb{Q}_ℓ (assume for the moment that $\ell \neq 2$). Then every element of T is conjugate in $\text{GL}_2(\mathbb{Q}_\ell)$ to $\begin{bmatrix} x & \epsilon y \\ y & x \end{bmatrix}$, and using (x, y) as the coordinates on T , the map ψ can be written as $\psi(x, y) = (x + \sqrt{\epsilon}y, x - \sqrt{\epsilon}y)$. Then one can simply compute

$$\psi^*\left(\frac{du}{u} \wedge \frac{dv}{v}\right) = 2\sqrt{\epsilon} \frac{dx \wedge dy}{x^2 - \epsilon y^2} = 2\sqrt{\epsilon} \omega_T.$$

Thus we get (for $\ell \neq 2$),

$$|c_T|_\ell = |2\sqrt{\epsilon}|_L = \begin{cases} 1 & L \text{ is unramified} \\ \sqrt{\ell} & L \text{ is ramified,} \end{cases}$$

which completes the proof of the lemma in the case $\ell \neq 2$.

There is, however, a better argument, which also covers the case $\ell = 2$. Namely, to find the ratio $\left| \frac{\omega_T}{\psi^*(\omega_{T^{\text{spl}}})} \right|_L$ of (4.4), we just need to find the ratio of the volume of $\mathcal{T}^\circ(\mathbb{Z}_\ell)$ with respect to the measure $|d\omega_T|$ to its volume with respect to $|d\psi^*(\omega_{T^{\text{spl}}})|$. This is, in fact, the same calculation as the one carried out in [22, p.22 (before Theorem 2.3.2)], and the answer is that the convergence factors for the pull-back of the form $\omega_{T^{\text{spl}}}$ to the restriction of scalars is $(\sqrt{|\Delta_K|_\ell})^{\dim(\mathbb{G}_m)}$, in this case. \square

Finally, summarizing the above discussion, we obtain

Proposition 4.5. *Let $\gamma \in \text{GL}_2(\mathbb{Q})$ be a regular element. Let T be the centralizer of γ , and let K be as in §2.1. Abusing notation, we also denote by γ the image of γ in $\text{GL}_2(\mathbb{Q}_\ell)$ for every finite prime ℓ . Then for every finite prime ℓ ,*

$$\mu_\gamma^{\text{geom}} = \frac{L_\ell(1, \xi_T)}{L_\ell(M_G^\vee(1))} |\Delta_K|_\ell^{-1/2} |D(\gamma)|_\ell^{1/2} \mu_\gamma^{\text{can}}$$

as measures on the orbit of γ .

5. THE GLOBAL CALCULATION

In this section, we put all the above local comparisons together, and thus show that Gekeler's formula reduces to a special case of the formula of Langlands and Kottwitz. In the process we will need a formula for the global volume term that arises in that formula. We are now in a position to give a new proof of Gekeler's theorem, and of its generalization to arbitrary finite fields.

Theorem 5.1. *Let q be a prime power, and let a be an integer with $|a| \leq 2\sqrt{q}$ and $\gcd(a, p) = 1$. The number of elliptic curves over \mathbb{F}_q with trace of Frobenius a is*

$$(5.1) \quad \#I(a, q) = \frac{\sqrt{q}}{2} v_\infty(a, q) \prod_{\ell} v_\ell(a, q).$$

Here, $v_\ell(a, q)$ (for $\ell \neq p$), $v_p(a, q)$, and $v_\infty(a, q)$ are defined, respectively, in (2.4), (2.6), and (2.7), and the weighted count $\#I(a, q)$ is defined in (2.1).

Proof. Recall the notation surrounding γ_0 and δ_0 established in §2.1. Given Proposition 2.1, it suffices to show that the right-hand side of (5.1) calculates the right-hand side of (2.8).

Let $G = \mathrm{GL}_2$. First, let

$$\phi^p = \otimes_{\ell \neq p} \mathbf{1}_{G(\mathbb{Z}_\ell)}$$

be the characteristic function of $G(\hat{\mathbb{Z}}_f^p)$ in $G(\mathbb{A}_f^p)$. The first integral appearing in (2.8) is equal to

$$O_{\gamma_0}(\phi^p) = \int_{G(\mathbb{A}^p)} \phi^p |d\omega_G| = \prod_{\ell \neq p} O^{\mathrm{can}}(\mathbf{1}_{G(\mathbb{Z}_\ell)}).$$

Combining Corollary 3.5, relation (4.2) and Proposition 4.5, we get, for $\ell \neq p$,

$$\begin{aligned} v_\ell(a, q) &= \frac{\ell^3}{\#G^{\mathrm{der}}(\mathbb{F}_\ell)} O_{\gamma_0}^{\mathrm{geom}}(\mathbf{1}_{G(\mathbb{Z}_\ell)}) = \frac{\ell^3}{\#G^{\mathrm{der}}(\mathbb{F}_\ell)} \frac{L_\ell(1, \xi_{T^{\mathrm{der}}})}{L_\ell(M_{G^{\mathrm{der}}}^\vee(1))} |\Delta_K|_\ell^{-1/2} |D(\gamma_0)|_\ell^{1/2} O_{\gamma_0}^{\mathrm{can}}(\mathbf{1}_{G(\mathbb{Z}_\ell)}) \\ &= L_\ell(1, \xi_{T^{\mathrm{der}}}) |D(\gamma_0)|_\ell^{1/2} |\Delta_K|_\ell^{-1/2} O_{\gamma_0}^{\mathrm{can}}(\mathbf{1}_{G(\mathbb{Z}_\ell)}). \end{aligned}$$

Second, let ϕ_q be the characteristic function of $G(\mathbb{Z}_p) \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} G(\mathbb{Z}_p)$ in $G(\mathbb{Q}_p)$, and let $\phi_{p,q}$ be the characteristic function of $G(\mathbb{Z}_q) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} G(\mathbb{Z}_q)$ in $G(\mathbb{Q}_q)$. Using Lemmas 3.6 and 3.7, we find that

$$\begin{aligned} v_p(a, q) &= \frac{p^3}{\#G^{\mathrm{der}}(\mathbb{F}_p)} O_{\gamma_0}^{\mathrm{geom}}(\phi_q) \\ &= \frac{p^3}{\#G^{\mathrm{der}}(\mathbb{F}_p)} \frac{L_p(1, \xi_{T^{\mathrm{der}}})}{L_p(M_{G^{\mathrm{der}}}^\vee(1))} |\Delta_K|_p^{-1/2} |D(\gamma_0)|_p^{1/2} O_{\gamma_0}^{\mathrm{can}}(\phi_q) \\ &= \frac{p^3}{\#G^{\mathrm{der}}(\mathbb{F}_p)} \frac{L_p(1, \xi_{T^{\mathrm{der}}})}{L_p(M_{G^{\mathrm{der}}}^\vee(1))} |\Delta_K|_p^{-1/2} |D(\gamma_0)|_p^{1/2} T O_{\delta_0}^{\mathrm{can}}(\phi_{p,q}). \end{aligned}$$

Taking a product over all finite primes, we obtain:

$$(5.2) \quad \prod_{\ell < \infty} v_\ell(a, q) = L(1, \xi_{T^{\mathrm{der}}}) \sqrt{\frac{|\Delta_K|}{|D(\gamma_0)|}} T O_{\delta_0}^{\mathrm{can}}(\phi_{p,q}) O_{\gamma_0}^{\mathrm{can}}(\phi^p).$$

Recall that $f_0(T)$, the characteristic polynomial of γ_0 , is $f_0(T) = T^2 - aT + q$. The (polynomial) discriminant of $f_0(T)$ and the (Weyl) discriminant of γ_0 are related by $|D(\gamma_0) \det(\gamma_0)| = |\mathrm{disc}(f_0)| = 4q - a^2$. Consequently,

$$\sqrt{q} v_\infty(a, q) = \frac{1}{\pi} \sqrt{|D(\gamma_0)|}.$$

Since $L(1, \xi_{T^{\mathrm{der}}}) = L(1, \xi_{T/\mathbb{Z}})$ (Lemma 4.2), (5.1) follows from (5.2) and Proposition 5.2 below, which is proved in the Appendix. \square

Proposition 5.2. *We have*

$$(5.3) \quad \frac{\sqrt{|\Delta_K|}}{2\pi} L(1, \xi_{T/Z}) = \text{vol}(T(\mathbb{Q}) \backslash T(\mathbb{A}_f)).$$

Proof. First, we note that $L(s, \xi_{T/Z})$ coincides with $L(s, K/\mathbb{Q})$, the Dirichlet L -function attached to the quadratic character of K . Now the proposition is obtained by combining Lemma A.5 with the analytic class number formula (A.6). \square

APPENDIX A. ORBITAL INTEGRALS AND MEASURE CONVERSIONS

S. Ali Altuğ

In this appendix we relate certain calculations of [2], initially intended for a different setting, to Gekeler's product formula (1.3). The strategy for the proof will follow the same lines as in the main text; the major differences are at the calculations of measure conversion factors and volumes. Since this appendix is to be complementary to the main text we will not aim for generality and simply take $q = p$, which is the case considered in [8]. More precisely, we will be proving:

Theorem. (*Theorem 5.1, $q = p$ -prime case*) Let p be a prime and let \mathbb{F}_p denote the finite field with p elements. Let $a \in \mathbb{Z}$ such that $|a| \leq 2\sqrt{p}$, $p \nmid a$ and let $I(a, p)$ denote the isogeny class of elliptic curves over \mathbb{F}_p with trace of their Frobenius equals a . For each finite prime ℓ , let $v_\ell(a, p)$ be the local probabilities defined by (1.1) and (1.2). Then

$$\#I(a, p) = \frac{\sqrt{4p - a^2}}{2\pi} \prod_{\ell \neq \infty} v_\ell(a, p).$$

The proof consists of four steps. The first two steps, relating $\#I(a, p)$ and the local densities to orbital integrals (with respect to different measures (!)), are the same as in the text, so instead of giving a detailed exposition of these we simply refer to the relevant parts of the article. The third step is to find the constant of proportionality in the two measure normalizations and to calculate the global volume factor that appears in the Langlands-Kottwitz formula, and the final step is to put everything together via the class number formula.

A.1. Steps 1 & 2: Sizes of isogeny classes, orbital integrals, and local densities.

A.1.1. Notation. Let $G := \mathrm{GL}_2$ and let \mathbb{A} be the adeles $\mathbb{A} = \mathbb{A}_{\mathbb{Q}}$. Following the notation of §3.2 and 3.3, for any prime $\ell \neq p$, let ϕ_0 denote the characteristic function of the $G(\mathbb{Z}_\ell)$. For $\ell = p$, let ϕ_p be the characteristic function of $G(\mathbb{Z}_p) \begin{pmatrix} p & \\ & 1 \end{pmatrix} G(\mathbb{Z}_p)$. Let $\gamma \in G(\mathbb{Q})$ be such that $\mathrm{tr}(\gamma) = a$ and $\det(\gamma) = p$. Note that since $a \in \mathbb{Z}$ and $|a| \leq 2\sqrt{p}$, γ is regular semisimple and its centralizer, G_γ , is a torus. Let us denote this torus by T . Finally, for any finite prime ℓ and $\phi \in C_c^\infty(G(\mathbb{Q}_\ell))$ let the orbital integrals $O_\gamma^{\mathrm{geom}}(\phi)$ and $O_\gamma^{\mathrm{can}}(\phi)$ be defined as in definitions 3.1 and 3.2 respectively. We remark that the difference between $O_\gamma^{\mathrm{geom}}(\phi)$ and $O_\gamma^{\mathrm{can}}(\phi)$ is in the chosen measure on the orbit of γ . Instead of going through the details of these measures we simply refer to Sections 2.2 and 3.1 of the paper as well as §3.3 of [7].

A.1.2. Sizes of isogeny classes to orbital integrals: Langlands-Kottwitz formula. For each finite prime ℓ let $d\mu_{G,\ell}^{\mathrm{can}}$ denote the measure on $G(\mathbb{Q}_\ell)$ normalized to give volume 1 to $G(\mathbb{Z}_\ell)$. On the centralizer $T(\mathbb{Q}_\ell) := G_\gamma(\mathbb{Q}_\ell)$ choose any measure $d\mu_{T,\ell}$. Let $d\bar{\mu}_\ell$ denote the quotient measure $d\mu_{G,\ell}^{\mathrm{can}}/d\mu_{T,\ell}$, and define $d\mu_{T,f} = \otimes_{\ell \neq \infty} d\mu_{T,\ell}$.

Proposition 2.1 combined with Lemma 3.7 states that

$$(A.1) \quad \#I(a, p) = \mathrm{vol}(\gamma, d\mu_{T,f}) \int_{T(\mathbb{Q}_p) \backslash G(\mathbb{Q}_p)} \phi_p(g^{-1}\gamma g) d\bar{\mu}_p(g) \prod_{\substack{\ell \text{ finite} \\ \ell \neq p}} \int_{T(\mathbb{Q}_\ell) \backslash G(\mathbb{Q}_\ell)} \phi_0(g^{-1}\gamma g) d\bar{\mu}_\ell(g),$$

where

$$(A.2) \quad \mathrm{vol}(\gamma, d\mu_{T,f}) := \int_{T(\mathbb{Q}) \backslash T(\mathbb{A}_f)} d\mu_{T,f},$$

and $\mathbb{A}_f = \prod'_{\ell \text{ finite}} \mathbb{Q}_\ell$ denotes the finite adeles. We also remark that the orbital integrals and the volume in (A.1) depend only on the conjugacy class of γ . Since, for semisimple elements, conjugacy in $G(\mathbb{Q})$ is equivalent to having the same characteristic polynomial (note that this uses the fact that $G = \mathrm{GL}_2$), (A.1) is well defined.

A.1.3. Orbital integrals to local densities. As in §A.1 fix a prime p , an integer $|a| \leq 2\sqrt{p}$, and $\gamma \in G(\mathbb{Q})$ such that $\mathrm{tr}(\gamma) = a$ and $\det(\gamma) = p$. Let the local densities $v_\ell(a, p)$ be defined by (1.1) and (1.2), and for any $\phi \in C_c^\infty(\mathbb{Q}_\ell)$ let $O_\gamma^{\mathrm{geom}}(\phi)$ be the orbital integrals, with respect to the geometric measure (cf. §2.2 and 3.1), defined as in definition 3.1. Then, recalling that $\#SL_2(\mathbb{F}_\ell) = \ell^3 \zeta_\ell(2)^{-1}$, Corollary 3.5 and Lemma 3.6 can be stated as

$$(A.3) \quad v_\ell(a, p) = \zeta_\ell(2) O_\gamma^{\mathrm{geom}}(\phi_0)$$

$$(A.4) \quad v_p(a, p) = \zeta_p(2) O_\gamma^{\mathrm{geom}}(\phi_p),$$

where ϕ_0 and ϕ_1 are as in §A.1, and $\zeta_\ell(s) = 1/(1 - \ell^{-s})$.

A.2. Step 3: Measure conversions and orbital integrals. Since the orbital integrals $O_\gamma^{\mathrm{geom}}(\phi)$ and $O_\gamma^{\mathrm{can}}(\phi)$ are defined with respect to different measure normalizations on the orbit of γ , in order to compare (A.3) and (A.4) to (A.1) we will need to relate integration against the quotient measure $d\bar{\mu}_\ell = d\mu_{G,\ell}^{\mathrm{can}}/d\mu_{T,\ell}$ to integration against $d\mu_\ell^{\mathrm{geom}}$. In order to do so, we start with a lemma that provides the conversion factor for a general quotient measure, $d\mu_{T \backslash G, \ell} := d\mu_{G, \ell}/d\mu_{T, \ell}$.

Lemma A.1. *Let ℓ be a finite prime, $\gamma \in G(\mathbb{Q})$, and $T = G_\gamma$ be as above. For any Haar measures $d\mu_{G, \ell}$ on G and $d\mu_{T, \ell}$ on T let $\mathrm{vol}(d\mu_{G, \ell})$ be the volume of $G(\mathbb{Z}_\ell)$ with respect to $d\mu_{G, \ell}$ and similarly let $\mathrm{vol}(d\mu_{T, \ell})$ denote the volume of $T(\mathbb{Z}_\ell)$. Let $d\mu_{T \backslash G, \ell}$ denote the quotient measure $d\mu_{G, \ell}/d\mu_{T, \ell}$. Let ω_G and ω_T be non-vanishing algebraic top degree forms on G and T respectively. Denote the measures associated to ω_G and ω_T by $|\omega_G|_\ell$ and $|\omega_T|_\ell$ respectively, and denote the induced quotient measure on $T \backslash G$ by $|\omega_{T \backslash G}|_\ell$. Finally, let $d\mu_{\gamma, \ell}^{\mathrm{geom}}$ be the geometric measure of §3.1.3 induced by ω_G . Then,*

$$d\mu_{\gamma, \ell}^{\mathrm{geom}} = \sqrt{|D(\gamma)|_\ell} \frac{\mathrm{vol}(|\omega_G|_\ell) \mathrm{vol}(d\mu_{T, \ell})}{\mathrm{vol}(|\omega_T|_\ell) \mathrm{vol}(d\mu_{G, \ell})} d\bar{\mu}_{T \backslash G, \ell},$$

where, by abuse of notation, $|D(\gamma)| = |\mathrm{tr}(\gamma)^2 - 4\det(\gamma)|$.

Proof. By equation (3.30) of [7], we have

$$d\mu_{\gamma, \ell}^{\mathrm{geom}} = \sqrt{|D(\gamma)|_\ell} |\omega_{T \backslash G}|_\ell,$$

where we note that the left hand side of (3.30) of loc. cit. is what we denoted by $d\mu_\gamma^{\mathrm{geom}}$. Here, we need to remind the reader that both measures are invariant under multiplication by central elements so without loss of generality we can assume that $G = G^{\mathrm{der}}$ (i.e. $D(\gamma) = D_{G^{\mathrm{der}}}(\gamma) \det(\gamma)$). On the other hand, since the Haar measure is unique up to a constant we have $|\omega_G|_\ell = c_\ell(G) d\mu_{G, \ell}$ and $|\omega_T|_\ell = c_\ell(T) d\mu_{T, \ell}$. The constants can be calculated easily by volumes of the integral points:

$$c_\ell(G) = \frac{\mathrm{vol}(|\omega_G|_\ell)}{\mathrm{vol}(d\mu_{G, \ell})} \quad \text{and} \quad c_\ell(T) = \frac{\mathrm{vol}(|\omega_T|_\ell)}{\mathrm{vol}(d\mu_{T, \ell})}.$$

Therefore, the quotient measures $d\bar{\mu}_{T \backslash G, \ell}$ and $|\omega_{T \backslash G}|_\ell$ are related by

$$|\omega_{T \backslash G}|_\ell = \frac{c_\ell(G)}{c_\ell(T)} d\bar{\mu}_{T \backslash G, \ell}.$$

The lemma follows. \square

As an immediate corollary to Lemma A.1 we get

Corollary A.2. *Let $d\mu_{G,\ell}^{can}$ and $d\mu_{T,\ell}^{can}$ be normalized to give measure 1 to $G(\mathbb{Z}_\ell)$ and $T(\mathbb{Z}_\ell)$ respectively, and let the rest of the notation be as in Lemma A.1. Then*

$$d\mu_{\gamma,\ell}^{geom} = \sqrt{|D(\gamma)|_\ell} \frac{\text{vol}(|\omega_G|_\ell)}{\text{vol}(|\omega_T|_\ell)} d\tilde{\mu}_{T \setminus G, \ell}.$$

We now quote a result of [17], where $\text{vol}(|\omega_G|_\ell)$ and $\text{vol}(|\omega_T|_\ell)$ are calculated for a specific pair of forms ω_G and ω_T . Let

$$(A.5) \quad \omega_G = \frac{d\alpha d\beta d\gamma d\delta}{\alpha\delta - \beta\gamma} \quad \text{and} \quad \omega_T = \frac{d\gamma_1 d\gamma_2}{\gamma_1 \gamma_2}$$

where we have chosen coordinates

$$G = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha\delta - \beta\gamma \neq 0 \right\}$$

$$T = \left\{ \begin{pmatrix} \gamma_1 & \\ & \gamma_2 \end{pmatrix} : \gamma_1 \gamma_2 \neq 0 \right\}.$$

Note that ω_G is the same form studied in Section 3.1.

Lemma A.3. *For ω_G and ω_T as in (A.5),*

$$\text{vol}(|\omega_G|_\ell) = \zeta_\ell(1)^{-1} \zeta_\ell^{-1}(2)$$

$$\text{vol}(|\omega_T|_\ell) = \sqrt{|\Delta_K|_\ell} \begin{cases} \zeta_\ell(1)^{-2} & K/\mathbb{Q} \text{ is split at } \ell \\ \zeta_\ell(2)^{-1} & K/\mathbb{Q} \text{ is unramified at } \ell, \\ \zeta_\ell(1)^{-1} & K/\mathbb{Q} \text{ is ramified at } \ell \end{cases}$$

where K/\mathbb{Q} is the quadratic extension where T splits over and Δ_K is the discriminant of K (so in the split and unramified cases $|\Delta_K|_\ell$ is 1).

Proof. The result for odd primes ℓ is given on pages 41 and 42 of [17]. The case for $\ell = 2$ follows the same lines. The only point to keep in mind is the extra factor of 2 that appears in the calculation of the differential form on page 42 of [17]; we leave the details to the reader. □

Corollary A.4. *Let the measure choices be as in Lemma A.3. Then for any $\phi \in C_c^\infty(G(\mathbb{Q}_\ell))$ and any regular semi-simple γ ,*

$$O_\gamma^{can}(\phi) = \frac{\sqrt{|\Delta_K|_\ell} \zeta_\ell(2)}{\sqrt{|D(\gamma)|_\ell} L_\ell(1, K/\mathbb{Q})} O_\gamma^{geom}(\phi).$$

Proof. By Lemma A.3 we have

$$\frac{\text{vol}(|\omega_G|_\ell)}{\text{vol}(|\omega_T|_\ell)} = \frac{1}{\sqrt{|\Delta_K|_\ell}} \begin{cases} \frac{1}{(1+1/q_\ell)} & \text{split} \\ \frac{1}{(1-1/q_\ell)} & \text{unramified} \\ (1-1/q_\ell^2) & \text{ramified} \end{cases} = \frac{L_\ell(1, K/\mathbb{Q})}{\sqrt{|\Delta_K|_\ell} \zeta_\ell(2)}.$$

The corollary then follows from Corollary A.2. □

The last step is to calculate the global volume term.

Lemma A.5. *Let (a, p) be such that $a^2 - 4p < 0$. Let $d\mu_{T,\ell}^{\text{can}}$ be the Haar measure normalized to give measure 1 to $T(\mathbb{Z}_\ell)$ and set $d\mu_{T,f}^{\text{can}} := \otimes_{\ell \neq \infty} d\mu_{T,\ell}^{\text{can}}$. Then,*

$$\text{vol}(\gamma, d\mu_{T,f}^{\text{can}}) = \frac{h_K}{w_K},$$

here K/\mathbb{Q} is the quadratic extension where T splits, w_K is the number of roots of unity in K , and h_K is its class number.

Proof. By identifying $T = G_\gamma$ with G_m over the quadratic extension K we have

$$\text{vol}(\gamma, d\mu_{T,f}^{\text{can}}) = \mu_{T,f}^{\text{can}}(T(\mathbb{Q}) \backslash T(\mathbb{A}_f)) = \mu_{K,f}^{\text{can}}(K^\times \backslash \mathbb{A}_{K,f}^\times),$$

where the measure on the right is such that $\mu_{K,f}^{\text{can}}(\mathcal{O}_v^\times) = 1$ for each place v . Let $\hat{\mathcal{O}}_K^\times = \prod_v \mathcal{O}_v^\times$. Recall that

$$1 \rightarrow (K^\times \cap \hat{\mathcal{O}}_K^\times) \backslash \hat{\mathcal{O}}_K^\times \rightarrow K^\times \backslash \mathbb{A}_{K,f}^\times \rightarrow \text{Cl}(K) \rightarrow 1,$$

which implies that $\mu(K^\times \backslash \mathbb{A}_{K,f}^\times) = h_K \mu((K^\times \cap \hat{\mathcal{O}}_K^\times) \backslash \hat{\mathcal{O}}_K^\times) = \frac{h_K}{w_K}$.

□

A.3. Proof of Theorem 5.1. Let us begin by recalling Dirichlet's class number formula for an imaginary quadratic field K/\mathbb{Q} :

$$(A.6) \quad L(1, K/\mathbb{Q}) = \frac{2\pi h_K}{w_K \sqrt{|\Delta_K|}},$$

where Δ_K the discriminant of K , w_K is the number of roots of unity in K , and h_K is its class number.

At this point the result essentially follows from a combination of Corollary A.4, Lemma A.5, and (A.6). We give the details:

By (A.1) we have

$$\tilde{\#}I(a, p) = \text{vol}_f(\gamma) O_\gamma^{\text{can}}(\phi_p) \prod_{\ell \neq p} O_\gamma^{\text{can}}(\phi_0).$$

Substituting Corollary A.4 and Lemma A.5 into the above equation (and noting that the product converges only conditionally so should be calculated in the given order) gives

$$\#I(a, p) = \frac{h_K}{w_K} \frac{\sqrt{|\Delta_K|_p} \zeta_p(2)}{\sqrt{|D(\gamma)|_p} L_p(1, K/\mathbb{Q})} O_\gamma^{\text{geom}}(\phi_p) \prod_{\ell \neq p} \frac{\sqrt{|\Delta_K|_\ell} \zeta_\ell(2)}{\sqrt{|D(\gamma)|_\ell} L_\ell(1, K/\mathbb{Q})} O_\gamma^{\text{geom}}(\phi_0).$$

Then, substituting (A.3) and (A.4), we get

$$\begin{aligned} \tilde{\#}I(a, p) &= \frac{h_K}{w_K} \prod_{\ell \text{ finite}} \frac{\sqrt{|\Delta_K|_\ell}}{\sqrt{|D(\gamma)|_\ell} L_\ell(1, K/\mathbb{Q})} v_\ell(a, p) \\ &= \frac{h_K}{w_K} \frac{1}{L(1, K/\mathbb{Q})} \prod_{\ell \text{ finite}} \frac{\sqrt{|\Delta_K|_\ell}}{\sqrt{|D(\gamma)|_\ell}} v_\ell(a, p). \end{aligned}$$

Finally, using (A.6) and the product formula (i.e. $\prod_{\ell} |\Delta|_{\ell} = \prod_{\ell} |D(\gamma)|_{\ell} = 1$, where the product is over *all* primes ℓ) in the above equation we get,

$$\begin{aligned} \#I(a, p) &= \frac{\sqrt{|\Delta_K|}}{2\pi} \frac{\sqrt{|D(\gamma)|}}{\sqrt{|\Delta_K|}} \prod_{\ell \text{ finite}} v_{\ell}(a, p) \\ &= \frac{\sqrt{4p - a^2}}{2\pi} \prod_{\ell \text{ finite}} v_{\ell}(a, p), \end{aligned}$$

where the absolute values $|\cdot|$ are the archimedean absolute values and we used the fact that $|D(\gamma)| = 4p - a^2$.

□

COLUMBIA UNIVERSITY, NEW YORK, NY

E-mail address: altug@math.columbia.edu

REFERENCES

- [1] Jeffrey D. Achter and Clifton L. R. Cunningham, *Isogeny classes of Hilbert-Blumenthal abelian varieties over finite fields*, J. Number Theory **92** (2002), no. 2, 272–303. MR1884704 (2002k:11089)
- [2] S. A. Altuğ, *Beyond Endoscopy via the Trace Formula-I: Poisson Summation and Isolation of Special Representations*, Compositio Mathematica **151** (2015), no. 10, 1791–1820.
- [3] Victor V. Batyrev, *Birational Calabi-Yau n -folds have equal Betti numbers*, New trends in algebraic geometry (Warwick, 1996), 1999, pp. 1–11. MR1714818 (2000i:14059)
- [4] Rony A. Bitan, *The discriminant of an algebraic torus*, J. Number Theory **131** (2011), no. 9, 1657–1671. MR2802140 (2012g:11118)
- [5] Laurent Clozel, *Nombre de points des variétés de Shimura sur un corps fini (d’après R. Kottwitz)*, Astérisque **216** (1993), Exp. No. 766, 4, 121–149. Séminaire Bourbaki, Vol. 1992/93. MR1246396 (95c:11075)
- [6] Chantal David, Dimitris Koukoulopoulos, and Ethan Smith, *Sums of Euler products and statistics of elliptic curves*, 2015. arXiv:1510.05935.
- [7] Edward Frenkel, Robert Langlands, and Báo Châu Ngô, *Formule des traces et fonctorialité: le début d’un programme*, Ann. Sci. Math. Québec **34** (2010), no. 2, 199–243. MR2779866 (2012c:11240)
- [8] Ernst-Ulrich Gekeler, *Frobenius distributions of elliptic curves over finite prime fields*, Int. Math. Res. Not. **37** (2003), 1999–2018.
- [9] Jayce Getz and Mark Goresky, *Hilbert modular forms with coefficients in intersection homology and quadratic base change*, Progress in Mathematics, vol. 298, Birkhäuser/Springer Basel AG, Basel, 2012. MR2918131
- [10] Benedict H. Gross, *On the motive of a reductive group*, Invent. Math. **130** (1997), 287–313.
- [11] Thomas C. Hales, *The fundamental lemma and the Hitchin fibration [after Ngô Bao Châu]*, Astérisque **348** (2012), Exp. No. 1035, ix, 233–263. Séminaire Bourbaki: Vol. 2010/2011. Exposés 1027–1042. MR3051198
- [12] Nicholas M. Katz, *Lang-Trotter revisited*, Bull. Amer. Math. Soc. (N.S.) **46** (2009), no. 3, 413–457. MR2507277
- [13] Robert E. Kottwitz, *Rational conjugacy classes in reductive groups*, Duke Math. J. **49** (1982), no. 4, 785–806. MR683003 (84k:20020)
- [14] ———, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc. **5** (1992), no. 2, 373–444. MR1124982 (93a:11053)
- [15] ———, *Harmonic analysis on reductive p -adic groups and Lie algebras*, Harmonic analysis, the trace formula, and Shimura varieties, 2005, pp. 393–522. MR2192014 (2006m:22016)
- [16] Robert P. Langlands, *Base change for $GL(2)$* , Annals of Mathematics Studies, 1980.
- [17] ———, *Singularités et transfert*, Ann. Math. Qué. **37** (2013), no. 2, 173–253. MR3117742
- [18] Gérard Laumon, *Cohomology of Drinfeld modular varieties, part I*, Cambridge University Press, 1996.
- [19] Peter Scholze, *The Langlands-Kottwitz approach for the modular curve*, Int. Math. Res. Not. IMRN **15** (2011), 3368–3425. MR2822177 (2012k:11090)
- [20] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.
- [21] Willem Veys, *Reduction modulo p^n of p -adic subanalytic sets*, Math. Proc. Cambridge Philos. Soc. **112** (1992), no. 3, 483–486. MR1177996 (93i:11142)
- [22] André Weil, *Adeles and algebraic groups*, Progress in mathematics, vol. 23, Birkhäuser.

COLORADO STATE UNIVERSITY, FORT COLLINS, CO

E-mail address: achter@math.colostate.edu

UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC

E-mail address: gor@math.ubc.ca